Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Department of Revenue; Disclosure
PROCEDURE #6.2.7	**SUBJECT:** Federal Incident Response and Reporting	
EFFECTIVE DATE: 10/24/15		
CONTACT: Disclosure Office		**LOCATION:** State Office Bldg; Station #6 **PHONE:** 502-564-2551 or 502-564-2552

STATEMENT OF AUTHORITY

1. The Finance and Administration Cabinet's Standard Procedures Manual establishes standard mandatory internal procedures cabinet-wide. These procedures are established in accordance with the Secretary's statutory authority under KRS 42.014 and KRS 12.270 to establish the internal organization and functions of the Cabinet as necessary to perform the duties effectively.

2. The Standard Procedures Manual may only be revised in accordance with the process outlined in Standard Procedure #1.1 entitled: "Finance Standard Procedures and Manual".

I. PURPOSE

Pursuant to KRS 131.190 and 26 USC 6103, incident response policy and procedures shall be developed, documented, disseminated and updated as necessary to facilitate the implementing incident response security controls. These policies and procedures shall cover both physical and information system security relative to the protection of federal tax information (FTI). Such incident response security controls include incident response training and incident reporting and monitoring.

II. INCIDENT RESPONSE

All personnel with access to federal tax information, including contractors and consolidated data center employees, if applicable, shall be trained in his/her incident response roles. Incident response training shall provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication and recovery. The Department of Revenue (DOR) shall routinely track and document all physical and information system security incidents potentially affecting the confidentiality of FTI. DOR shall test and/or exercise the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results by following the Internal Revenue Service (IRS) Safeguards Technical Assistance Memorandum Incident Response Test and Exercise Guidance maintained in the Disclosure Office.

III. INCIDENT RESPONSE PROCEDURE

A. DOR employees who suspect or have knowledge of a compromise to FTI shall

immediately notify his/her supervisor or the Disclosure Office.

1. In the instance the supervisor is notified, the supervisor shall immediately notify the Disclosure Office.

2. The Disclosure Office must immediately report incident information to the Office of the Commissioner and to the appropriate Agent-in-Charge, U.S. Treasury Inspector General for Tax Administration (TIGTA) and the IRS.

3. In addition, all federal breaches of information must all be reported to the proper state agency pursuant to KRS 61.933(1)(a)(1).

B. IRS OFFICE OF SAFEGUARDS NOTIFICATION PROCESS

1. Simultaneously to notifying TIGTA, the agency must notify the IRS Office of Safeguards. The TIGTA contact information is: Chicago TIGTA Field Division (312) 886-0620 extension 104.

2. To notify the IRS Office of Safeguards, the agency should document the specifics of the incident known at that time into a Data Incident Report, including but not limited to:

   a. Name of agency and agency point of contact for resolving data incident with the contact information.

   b. Date and time of the incident.

   c. Date and time the incident was discovered.

   d. How the incident was discovered.

   e. Description of the incident and the data involved, including specific data elements, if known.

   f. Potential number of FTI records involved. If unknown, provide a range, if possible.

   g. Address where the incident occurred.

   h. Information technology involved (e.g., laptop, server, mainframe).

i. Do not include any FTI in the Data Incident Report.

j. Email the Data Incident Report to the SafeguardReports@IRS.gov mailbox. Reports should be sent electronically and encrypted via IRS approved encryption techniques. Use the term "Data Incident Report" in the subject line of the email.

Note: Timely notification is the most important factor, not the completeness of the Data Incident Report. Additional information will be secured via conversations with the IRS Office of Safeguards.

C. POST INCIDENT REVIEW

1. The agency will conduct a post-incident review to ensure the incident response policies and procedures provided adequate guidance.

2. Any identified deficiencies in the incident response policies and procedures should be resolved immediately.

3. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees immediately.

D. INCIDENT RESPONSE TIMEFRAMES

1. The agency will contact TIGTA and the IRS immediately, but no later than 24 hours after identification of a possible issue involving FTI.

2. The agency should not delay contacting TIGTA and the IRS to conduct an internal investigation to determine if FTI was involved.

3. If FTI was definitely involved, the agency must contact TIGTA and the IRS immediately.

E. INCIDENT RESPONSE COOPERATION

1. The agency will cooperate with TIGTA and the IRS Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

2. Based upon the analysis of the incident, the agency may be required by the IRS

Office of Safeguards to modify security policy, procedure or controls to more appropriately protect FTI in the possession of the agency.

3. The IRS Office of Safeguards will coordinate with the agency to ensure appropriate follow-up actions taken by the agency have been completed to ensure continued protection of FTI in the possession of the agency.

F. INCIDENT RESPONSE NOTIFICATION TO IMPACTED INDIVIDUALS

1. Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the agency's internal policy since the FTI is within the agency's possession or control.

2. However, the agency must inform the IRS Office of Safeguards of notification activities undertaken, preferably before released to the impacted individuals. In addition, the agency must inform the IRS Office of Safeguards of any pending media releases, including sharing the text prior to distribution.

IV. DISCLOSURE OFFICE CONTACT

Contact the DOR's Disclosure Officer at:

Department of Revenue
501 High Street
PO Box 1229, Station #6
Frankfort, KY 40602-1229

Telephone number: *502-564-2552* or *502-564-2551*

Fax number: *502-564-9896*

V. DISCIPLINARY ACTION

Failure to adhere to the statutory requirements of KRS 131.190 is punishable by those penalties found in KRS 131.990(2), including reprimand, suspension or dismissal.

Failure to adhere to the statutory requirements of 26 USC 6103(a)(2) or 26 USC 7213A is punishable by those penalties found in 26 USC 7213, 26 USC 7213A and 26 USC 7431 including reprimand, suspension or dismissal.

VI. REFERENCE

Publication 1075 Section 9.9 IRS Safeguards Technical Assistance Memorandum Incident Response and Incident Reporting

KRS 61.933: Notification of personal information security breach -- Investigation -- Notice to affected individuals of result of investigation -- Personal information not subject to requirements -- Injunctive relief by Attorney General